RUSSELL J. FRACKMAN (State Bar No. 49087)
PATRICIA H. BENSON (State Bar No. 60656)
STEVEN B. FABRIZIO (*pro hac vice*)
MITCHELL SILBERBERG & KNUPP LLP
11377 West Olympic Boulevard
Los Angeles, CA 90064-1683
Telephone: (310) 312-2000
Facsimile: (310) 312-3100

Attorneys for Defendants and Counterclaimants

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

321 STUDIOS, also known as 321 Studio, LLC, Plaintiff, v. METRO-GOLDWYN-MAYER STUDIOS INC.; TRISTAR PICTURES, INC.; COLUMBIA PICTURES INDUSTRIES, INC.; SONY PICTURES ENTERTAINMENT, INC.; TIME WARNER ENTERTAINMENT CO. L.P.; DISNEY ENTERPRISES, INC.; UNIVERSAL CITY STUDIOS, INC.; and THE SAUL ZAENTZ COMPANY, Defendants.	Case No.: C 02-1955-SI **DECLARATION OF ROBERT W. SCHUMANN IN SUPPORT OF MOTION OF DEFENDANTS AND COUNTERCLAIMANTS FOR PARTIAL SUMMARY JUDGMENT** Date: February 28, 2003 Time: 9:00 a.m. Courtroom: 10, 19th Floor Judge: Hon. Susan Illston
METRO-GOLDWYN-MAYER STUDIOS INC.; TRISTAR PICTURES, INC.; COLUMBIA PICTURES INDUSTRIES, INC.;TIME WARNER ENTERTAINMENT COMPANY, L.P.; DISNEY ENTERPRISES, INC.; UNIVERSAL CITY STUDIOS LLLP, formerly known as UNIVERSAL CITY STUDIOS, INC.; and THE SAUL ZAENTZ COMPANY, Counterclaimants, v. 321 STUDIOS, also known as 321 Studio, LLC,; ROBERT MOORE, an individual; ROBERT SEMAAN, an individual; and VICTOR MATTISON, an individual, Counterclaim Defendants.	

I, Robert W. Schumann, declare as follows:

1. I am the President and Chief Executive Officer of Cinea, Inc. Cinea is a digital content security firm that creates and develops security systems, with a focus on measures to protect digital content -- particularly motion picture content. My curriculum vitae is attached hereto as Exhibit A. The observations and conclusions set forth below are based upon my specialized knowledge, education and experience regarding digital video formats and content protection measures, including those at issue in this case. It also is based upon my review and analysis of relevant documents and other things, including the software applications entitled "DVD Copy Plus" and "DVD-X-Copy." If called as a witness in this action, I could and would competently testify to the following.

2. I have worked in the computer and information technology industry for the past 18 years. In 1985, I received a Bachelor of Science in Computer Science from Rochester Institute of Technology. Since that time, I have worked in various facets of the computer industry, including in connection with the development and design of computer network systems, computer software, and digital security systems.

3. I have been involved in designing, developing, and implementing security systems for digital content (including digital cinema and video) for the past nine years. Prior to founding Cinea, I was responsible for the development and implementation of a technology known as Divx. Divx was a highly sophisticated system that enabled the secure transmission, receipt, and viewing of digital video content delivered on DVD disc. Among the work I performed in connection with Divx was the creation and development of a content security system that would enable the producers of video or creative content to license or distribute their content on DVDs without undue risk of piracy or unauthorized access.

4. In or about July 2000, I testified as an expert witness at trial in the action entitled Universal City Studios, Inc. v. Reimerdes, Case No. 00-Civ-0277 (LAK) (S.D.N.Y.). This case involved the distribution of DVD copying software known as "DeCSS," which is described in detail below. In connection with the Reimerdes action, the Court accepted my qualifications to testify as an expert witness.

5. I have conducted analyses and evaluations of two software products that I am informed are manufactured and distributed by 321 Studios ("321"): DVD Copy Plus and DVD-X-Copy. I was provided with retail CD copies of both software applications and, in addition, directed the purchase and downloading of copies through 321's Internet web site. I undertook to operate, and supervised the operation of, both DVD Copy Plus and DVD-X-Copy to duplicate several motion picture DVDs. True and correct copies of the retail packaging for the DVD Copy Plus and DVD-X-Copy software on which I performed my analyses are attached hereto, respectively, as Exhibits B and C.

6. My principal findings and conclusions, explained in more detail below, are the following:

a. Both DVD Copy Plus and DVD-X-Copy circumvent the protection system known as "CSS," which is incorporated into nearly all commercially released motion picture DVDs. Specifically, these programs circumvent the access control and copy protections afforded by CSS and its encryption mechanisms.

b. During operation, DVD Copy Plus and DVD-X-Copy create or cause to be created decrypted, unprotected (or "plain text") copies of the contents of an original DVD on a user's computer hard drive and on recordable CDs or DVDs. Those "plain text" copies can be further copied, distributed or otherwise manipulated in the same manner as any other unprotected computer files.

DVD Technology

7. The term DVD is an acronym for "Digital Versatile Disc." It describes a high capacity digital storage medium, as well as a family of "standards" that describe how to store and read content on DVD discs. DVDs are similar in physical shape and size to the storage medium known as the CD, or compact disc, which is the familiar digital medium used to store digital audio content.

8. Depending on its configuration, a DVD can store up to a maximum of 18 gigabytes of data. In its most common deployment for motion pictures, a DVD will hold approximately 9 gigabytes of data. By comparison, a typical audio CD will store about 700 megabytes of data. Since one gigabyte equals 1024 megabytes, a 9 gigabyte DVD holds many times more data - - more than 12 times more data - - than a 700 megabyte CD.

9. Because of their enormous storage capacity, DVDs are able to store the digital content that comprises a full-length motion picture. Subject to the security and encryption restrictions discussed below, DVDs are viewable either on a television using a stand-alone DVD player or on a computer with a DVD drive and specialized playback software, known as DVD player software.

10. DVDs have become very popular for the private home viewing of recorded motion pictures. As compared to video cassettes (or VCR tapes), DVDs offer dramatically improved audio and visual quality. Since the commercial introduction of the DVD in 1997, more than 5000 major motion pictures have been released on DVD format, and more than 35 million stand-alone DVD players have been sold in the United States. Most mid-level and higher-end computers now come standard with DVD drives and DVD player software.

11. There is, however, a downside to the digital format. When a motion picture or other video content has been converted to digital format, there is a greatly enhanced risk of unauthorized reproduction and distribution. This is because, unlike with analog formats, such as a VCR tape, when material is copied digitally, the quality of the copy does not degrade from generation to generation (for example, from DVD copy to DVD copy). In other words, a second, third or fourth generation copy is identical in quality to the original. Also, once a motion picture has been converted to digital format, it easily can be distributed using portable media (such as DVD discs) or electronically, over the Internet. This allows pirate copies to proliferate exponentially, frustrating enforcement efforts. Absent some form of protection, the digital content on DVDs would be vulnerable to such unauthorized reproduction and distribution.

The Development and Operation of CSS

12. Because of the concern about unauthorized reproduction and distribution of motion pictures on DVDs, in the early 1990s, the motion picture companies made the development of an access control and copy prevention system an integral part of the development of the DVD format. This system was developed by Matsushita Electric Industrial Co. Ltd. and Toshiba Corporation and became known as "CSS" (which stands for "Content Scramble System"). The CSS standard ultimately was adopted by motion picture companies as the standard for video protection on DVDs and has been widely adopted by manufacturers of consumer electronics and computer devices.

13. CSS technology is licensed to manufacturers by an organization known as the DVD Copy Control Association ("CCA"). CCA controls all licensing of CSS technology and issues licenses to manufacture CSS-compliant devices. CSS has been licensed to hundreds of DVD player manufacturers (both hardware and software) and DVD content distributors in the United States and around the world.

14. CSS protects the contents of a DVD both from unauthorized access and from unauthorized copying. The mechanics of CSS differ slightly depending on whether the environment is a stand-alone DVD player or a personal computer. Because the 321 applications operate in the personal computer environment, I will limit my discussion herein to CSS as it operates in the personal computer environment. To protect DVD content, CSS relies on an integrated system of access "locks," encryption technology and licensing provisions, as follows:

a. First, CSS provides for a "locking" mechanism whereby a computer's DVD drive will not allow access to the CSS-protected content on a DVD disc unless and until the DVD drive has confirmed that the DVD player seeking access is an authentic, CCA-licensed DVD player. If the DVD player software does not contain the proper authentication, indicating to the DVD drive that it is "safe" to release the DVD data, the contents of the DVD will remain locked in the DVD drive. This means that the computer will not be able to "read" the CSS-protected content - - whether for purposes of playing the DVD, copying it, or otherwise.

b. Second, CSS uses encryption technology to scramble the digital data that makes up each frame of a DVD video stream. Only CCA-licensed DVD players are given access to the decryption keys needed to unscramble those images. The encryption of the DVD data is a level of security above and beyond the access control described above. Thus, even if one were to defeat the control on access – and somehow cause the DVD drive to release the DVD contents – those contents themselves would be protected (through encryption). No copy made of the scrambled contents would be playable or viewable unless de-scrambled. Authorized de-scrambling requires a combination of the original DVD disc in the computer's DVD drive and CCA-licensed DVD player software.

c. Third, CCA licenses CSS subject to strict requirements that prevent misuse of the DVD content by licensed players. For example, the license terms include provisions prohibiting authorized DVD players from permitting the copying of DVDs and requiring that CSS technology be maintained as confidential. These controls are intended to ensure that CSS does not become generally available and that DVD player technology is used only to enable viewing – and not copying – of DVDs.

15. Here is a simplified overview of how CSS works in practice. A user places a CSS-protected DVD movie into the DVD drive of her computer and opens DVD player software to view the movie. Internally, this results in a recognition by the DVD player that the disc is protected. This, in turn, initiates a series of communications between the DVD player and drive – an authentication process – through which the drive determines if the DVD player software is properly CCA-licensed. If the player is authentic, the process continues. If not, the DVD drive returns an error message and neither the player software nor any other application will be permitted to read the protected contents of the DVD disc. The DVD drive would remain "locked" and the protected DVD contents could not be played, copied or accessed at all. Assuming the DVD player software is determined to be an authentic, CCA-licensed player, then the DVD drive would unlock, allowing access to the DVD data. This authentication/unlocking sequence is repeated anew each time a DVD disc is inserted in the drive (even if the disc has previously been played).

16. Unlocking the drive gives access to the DVD data, but because that data is encrypted, it cannot be viewed until it is first decrypted. In order to decrypt the DVD data, the player software needs the appropriate decryption keys. The process of decrypting the DVD content involves multiple levels of encryption and decryption, all with the aim of making sure that the ultimate “keys” that will decrypt the DVD audio-video content – and thus the content itself – will remain secure. There are four critical sets of decryption keys: one is known as the "disc key"; a second set of keys are called “title keys”; a third set of keys are called “session keys”; and the fourth set of keys are “player keys.” Both the “disc key” and the “title keys” are stored in secure areas on the DVD disc, and are themselves encrypted. The “disc key” (when

decrypted as explained below) is used to decrypt the "title keys." The "title keys" are used to decrypt the actual DVD content. Individual "player keys" are assigned by CCA to the manufacturers of CCA-licensed DVD players, and are maintained securely in the DVD player software. The player keys are used by the DVD player to decrypt the disc key. Both the DVD drive and the DVD player, using mathematical algorithms during the authentication process, independently generate a common "session key." A given session key is unique to that DVD viewing session and is deleted whenever the DVD disc is removed or the DVD player software is closed. A different unique session key is generated for each subsequent viewing session. The session key is used to add a second layer of encryption (a "super-encryption") to the disc key and the title keys before those keys are communicated from the DVD drive to the DVD player.

17. In short, the process proceeds as follows: once the DVD player software has been authenticated, the DVD drive reads a block of data containing encrypted disc keys from the disc. It then super-encrypts the disc key block with a second layer of encryption using the then-current session key and communicates the twice-encrypted disc key block to the DVD player. The DVD player uses its copy of the then-current session key to decrypt the disc key block's outer layer of encryption. The DVD player then uses its CCA-assigned player keys to decrypt the individual disc key.

18. A DVD disc may contain any number of audio-video titles. The featured movie will be a title. The DVD may also contain, for example, several movie trailers or previews, or interviews with the cast or director. Each of these would be separate audio-video titles. There may be dozens of separate titles on a major motion picture DVD. Each may have its own title key. Once the user has selected the title she wants to view, the DVD player requests the appropriate title key from the DVD drive. The DVD drive responds by reading the title key for the selected title, encrypting that title key with a second layer of super-encryption using the current session key, and then communicating that twice-encrypted title key to the DVD player. The player decrypts the outer layer of encryption using its session key, and then uses the

previously-decrypted disc key to decrypt the title key. With the fully-decrypted title key, the DVD player can decrypt, and enable viewing of, the CSS-protected DVD content for that title.

19. Once the DVD player has decrypted the disc and title keys, those keys, along with the current session key, are stored by the DVD player software in a temporary memory location. The keys are maintained by the DVD player only for a single viewing session. When the DVD player software is closed, or the DVD disc is removed, the session ends and the keys are deleted. Even if the same DVD disc is immediately reinserted into the DVD drive, the entire process of player authentication and "key" communication and decryption needs to start again from the beginning.

20. Only after "unlocking" the DVD drive, and obtaining all necessary decryption keys, can a CCA-licensed DVD player access (read) and decrypt the DVD contents. By terms of the CCA license, DVD players are prohibited from copying, or enabling the copying of, the DVD disc or the decrypted audio-video data stream that it produces. A CCA-licensed player can only enable viewing of the DVD movie.

21. To the user seeking to view a DVD movie using an authorized player, the above CSS process is invisible and nearly instantaneous. However, as a result of the multiple levels of protection embodied in CSS, CSS-protected DVDs cannot be accessed or played on noncompliant players and cannot be copied (including on a personal computer).

DeCSS Decryption Technology

22. Sometime in 1999, I learned that a software utility known as “DeCSS” had appeared on the Internet (presumably, the first syllable refers to the program's ability to “de-scramble” or “de-crypt” CSS). In late-1999, I was retained by the Motion Picture Association of America, on

behalf of several motion picture studios, to perform an analysis and investigation into the origins and operation of DeCSS.

23. Based upon my research into DeCSS at that time, I determined that DeCSS is a software program that performs a single function -- the removal of CSS protection from a DVD in order to allow the copying of otherwise protected DVD contents. From the user's perspective, the process is simple. The DeCSS-user places the CSS-protected DVD into her computer's DVD drive, selects the files from the DVD to be copied onto the hard drive, and then presses a button to write (or copy) the files. After the completion of the DeCSS process, the user is left with an unencrypted, unprotected (or, as known in the computer security field, "plain text") set of files containing the contents of the original DVD on her computer hard drive. The quality of the resulting decrypted movie is identical to that of the encrypted movie on the original DVD. Because all of the CSS protections have been stripped away, the resulting files can be played on any DVD player, and can be further copied to recordable DVDs or distributed at will.

24. DeCSS circumvents the CSS protections by mimicking the CSS functions performed by an authorized CCA-licensed DVD player. DeCSS, in part, was created by "reverse engineering" CCA-licensed DVD players to obtain the player authentication sequence, the player keys, the necessary algorithms for generating the "session keys," and the CSS encryption algorithm itself. Thus, DeCSS is able to trick DVD drives into believing that the DeCSS software is a CCA-licensed DVD player. In doing so, DeCSS is able to "unlock" the DVD drive to gain access to the DVD contents. It also is able to obtain the DVD's various decryption keys, thus enabling it to de-scramble the DVD contents. The end result is that DeCSS creates an unprotected, plain text copy of the DVD contents on a user's computer hard drive.

The 321 Software

25. Analysis and testing of 321's software products, DVD Copy Plus and DVD-X-Copy, reveal that they accomplish the same circumvention as DeCSS, and appear to do so in substantially the same way. Using each piece of software, I successfully was able to copy CSS-protected motion picture DVDs, including "You've Got Mail" and "Harry Potter And The Sorcerer's Stone." I have confirmed that both 321 applications operate to circumvent CSS by improperly obtaining access to the DVD's contents, decrypting the contents of the DVD, and copying those decrypted contents to a user's computer hard drive in an unprotected, plain text format. My specific findings are described below.

DVD Copy Plus

26. DVD Copy Plus is a software package that enables a user to copy a CSS-protected DVD onto a recordable CD (also known as a CD-R). It does this in three phases: (1) it copies the contents of a CSS-protected DVD onto the computer's hard drive in an unprotected, plain text format; (2) to accommodate the much smaller capacity of a CD, it shrinks the size of the resulting files through a process known as "compression"; and (3) it copies (or burns) the compressed plain text files from the hard drive onto a CD-R.

27. DVD Copy Plus is packaged as one piece of software, but it is readily apparent from using the software that it is in fact three separate software applications "bundled" together by 321. The three applications are: "SmartRipper," "DVDx," and "PowerCDR." I am familiar with, and have used, each of these applications, as they are freely available over the Internet. The functions performed by the three applications correspond to the three phases described above. SmartRipper accesses the contents of a CSS-protected DVD, de-scrambles the contents, and copies the unprotected, plain text contents onto a computer hard drive. (The process of copying from a disc to a hard drive often is referred to as "ripping"; hence the name

SmartRipper). DVDx is a compression application. It reduces the size of the files on the hard drive so the contents of a DVD will fit onto a standard CD-R. PowerCDR is CD "burning" software; it copies the compressed files from the hard drive onto a CD-R. In essence, 321 has bundled these three software applications together and overlaid them with a relatively simple program. This program includes a tutorial that "walks" the user, step-by-step, through each of the programs, as well as a "launch menu" which allows the user to quickly access each program. True and correct copies of "screenshots" of DVD Copy Plus in use are attached hereto, collectively, as Exhibit D.

28. I have been familiar with SmartRipper for some time; descriptions of its operations, downloadable versions, and other documentation are widely available over the Internet. SmartRipper is built upon, and operates in a manner largely identical to, DeCSS – that is, SmartRipper circumvents CSS by mimicking a CCA-licensed DVD player. By pretending to be a CCA-licensed DVD player, SmartRipper unlocks the DVD drive, obtains the necessary CSS decryption keys, uses those keys to decrypt the DVD's contents, and then copies, in an unprotected format, the DVD's audio and video files to the user's computer hard drive.

29. My analysis and testing of SmartRipper demonstrates that SmartRipper either uses the core of the DeCSS software or operates in a manner substantially similar to DeCSS. This conclusion is based on the following:

a. My analysis of SmartRipper and related public documentation. My use and analysis of SmartRipper and review of public documentation pertaining to SmartRipper confirms that SmartRipper performs the same access, decryption, and copying functions as DeCSS, and does so in the same or substantially the same way.

b. My observations of the SmartRipper software in operation. While SmartRipper was operating to copy the contents of my CSS-protected DVD, it displayed a window entitled "Code Info." The "Code Info" window displayed the CSS "title key" for the DVD being copied, as well as the progress of the decryption process. Thus, my observation confirmed that SmartRipper (1) had extracted the relevant CSS decryption keys; (2) was using these keys to unscramble the DVD's contents, and (3) was copying onto my computer hard drive an unencrypted copy of the motion picture. A true and correct copy of a screenshot reflecting the above is attached hereto as Exhibit E.

c. My review of the results of the SmartRipper process. After "SmartRipper" had completed its operation on my CSS-protected DVD, it created a series of files on my hard drive that I confirmed were decrypted versions of the media contained on the DVD. I was able to play the files on my hard drive using standard DVD player software after removing the original DVD disc from my computer's DVD drive. Because the necessary CSS keys must be read from the original DVD disc itself, I would not have been able to play the copied DVD contents unless the CSS protection had been first stripped away.

30. CSS was designed to prevent -- and, in the normal course of its operation, does prevent -- access to the protected content on a DVD in the absence of a CCA-licensed player, unauthorized decryption of the DVD content, and the copying of the DVD content. 321's DVD Copy Plus software circumvents each of these CSS protections.

DVD-X-Copy

31. Whereas DVD Copy Plus copies CSS-protected DVDs onto CD-Rs, DVD-X-Copy enables the user to copy CSS-protected DVDs onto recordable DVDs (also known as DVD-Rs). Because DVD-X-Copy is copying from a DVD to a DVD-R, it does not need to shrink (or compress) the file size. Thus, DVD-X-Copy consists of two main operational functions: a function to copy (or "rip") the contents of a CSS-protected DVD to a user's hard drive, and a second function to copy (or "burn") the DVD's contents from a user's hard drive to DVD-Rs.

32. The ripping and circumvention component for DVD-X-Copy appears to be proprietary to 321. Thus, unlike with SmartRipper, I have not been able to analyze publicly available implementation information. Nevertheless, through observations of the DVD-X-Copy application in operation and through other testing, I have been able to confirm the functions performed by DVD-X-Copy.

33. My principal conclusion is that DVD-X-Copy functions in a manner similar to DVD Copy Plus and DeCSS. By that I mean, DVD-X-Copy is able to gain access to the otherwise "locked" contents on a DVD disc; it is able to copy the contents of the DVD onto the user's computer hard drive; and the copy stored on the user's hard drive is decrypted and stripped of its CSS protection. When DVD-X-Copy burns that de-scrambled content to a DVD-R, the resulting DVD-R also is de-scrambled and can be played in any DVD player. Thus, DVD-X-Copy accesses and de-scrambles CSS-protected DVD content, copies the de-scrambled content onto a computer hard drive, and further copies that unprotected content to DVD-R.[1] Absent the use of DVD-X-Copy, the ordinary operation of CSS would prevent the access, de-scrambling and copying of that DVD content.

34. My conclusions are based on the following observations and testing:

a. First, I began with a "clean" computer – one containing a completely blank, reformatted hard drive, with no programs or applications on it at all. I installed onto that computer only the Windows XP operating system. I did not install any other software applications, and confirmed that no other software applications were present on the

[1] When it writes the de-scrambled contents of a DVD to a user's computer hard drive, DVD-X-Copy places those contents in a "temporary" storage file. While in the normal course, those copied files on the hard drive are deleted after DVD-X-Copy copies them onto DVD-Rs, it is a trivial matter, using any number of standard Windows utilities, to move those de-scrambled files, stripped of CSS, to a permanent storage area on the user's computer. Once moved, the files will not be deleted and subsequently may be distributed or copied onto DVD-Rs any number of times.

computer's hard drive. Specifically, the testing computer did not contain DVD player software of any kind, and was not equipped to play any DVD, whether CSS-protected or otherwise.

b. Second, I inserted into the DVD drive a commercially released DVD motion picture, "Harry Potter And The Sorcerer's Stone," which is protected by CSS. I confirmed that no software application on the testing computer was capable of accessing, playing or copying the contents of that DVD. I attempted to play the DVD. That attempt was unsuccessful. I attempted to access the DVD's contents and copy them to my computer's hard drive using standard Windows utilities. As would be expected with a CSS-protected DVD, while I could see a listing of the files on the DVD, I was not able to access or copy those files onto my computer.

c. Third, I installed the DVD-X-Copy software onto the computer.

d. Fourth, I followed the DVD-X-Copy instructions and on-screen prompts in an effort to copy the same DVD in the DVD drive. After selecting the files I wished to copy, I clicked a button labeled "Copy Now." I then observed that DVD-X-Copy began to copy each of these files to my computer's hard drive. During the copying process, a window appeared on my computer screen indicating that DVD-X-Copy was "preparing" the files for copying. DVD-X-Copy also displayed a "progress" bar, indicating its progress in copying the DVD's content. As DVD-X-Copy was copying the DVD, I could see the light on my DVD drive go on (indicating activity) and I could hear activity both on my DVD drive and on my hard drive. DVD-X-Copy also has a video "preview" feature, which allowed me to observe the de-scrambled video prior to copying it. (The purpose of this "preview" feature is to allow the user, in instances in which the copied motion picture is too large to fit on a single DVD-R, to select the point at which the motion picture is to be divided between DVD-R discs). The fact that I was able to view a "preview" of the DVD motion picture confirmed that DVD-X-Copy had in fact decrypted the DVD. True and correct copies of pictures of my computer screen during the process of operating DVD-X-Copy as described above are attached hereto as Exhibit F.

e. Finally, before completing the DVD-X-Copy operation, I examined the contents of my hard drive and located a series of files that contained the DVD contents that had been copied. In order to confirm that these files were not encrypted, I transferred them to a second computer which contained a DVD player. I was able to view the DVD movie (together with the menus and "extras") without placing the original DVD in the computer's DVD drive. Additionally, I was able to play the contents of the DVD-R copy made with the DVD-X-Copy software on a stand-alone DVD player. In both cases, this would not have been possible unless the copy that resulted from the operation of DVD-X-Copy was de-scrambled and stripped of its CSS protection.

35. From this analysis, I can verify the following conclusions:

a. The operation of DVD-X-Copy enables a user to access the otherwise "locked" content on a CSS-protected DVD disc. This is apparent from the fact that I was unable to access the files on the DVD disc prior to installing DVD-X-Copy, but was able to do so using DVD-X-Copy.

b. The operation of DVD-X-Copy causes the de-scrambling of the contents of a CSS-protected DVD. This is necessarily true because no other application on my testing computer was capable of, or could be used to, decrypt or de-scramble the contents of a CSS-protected DVD. Indeed, prior to installing the DVD-X-Copy software, I specifically tried to play or view the DVD, and could not. The DVD-X-Copy software resulted in a copy of the DVD contents, in plain text, stripped of its CSS protection. The DVD-X-Copy software also allowed me to preview the DVD's video content in its de-scrambled form. Only the operation of the DVD-X-Copy software could have caused the de-scrambling of the DVD content.

c. The operation of DVD-X-Copy results in a copy of the DVD contents, de-scrambled and stripped of CCS, being made onto the hard drive of a user's computer. Moreover, the DVD-Rs made from DVD-X-Copy also are de-scrambled and stripped of CSS protection. This is apparent because both the hard drive copy and the DVD-R copy could readily be played with CCA-licensed DVD players – which would not be possible if the contents had been scrambled or otherwise retained their CSS protection.

36. Because a DVD drive will not "unlock" the contents of a CSS-protected DVD until it has authenticated the application seeking access as an authorized, CCA-licensed DVD player, I can conclude that DVD-X-Copy gains access to the DVD contents by somehow mimicking an authorized, CCA-licensed player – either using the DeCSS code itself or some process similar to DeCSS or SmartRipper. However, irrespective of how DVD-X-Copy specifically accomplishes it, one conclusion is inescapable: DVD-X-Copy circumvents the normal DVD access and copy protections afforded by CSS.

37. I also have assessed the claim made by 321 that DVD-X-Copy will not allow serial copying – meaning that it will copy an original DVD, but will not copy a DVD-R copy that has been made from that original. My observations are that the DVD-X-Copy software in fact will not make a second generation (or serial) copy of a DVD-R that originally was made using DVD-X-Copy. This is because DVD-X-Copy puts a “marker” file on the DVD-Rs it creates. If that marker is present, DVD-X-Copy will not make a serial copy of that DVD-R. However, this does little to prevent serial copying. Only DVD-X-Copy (and no other software) will recognize the “marker” file. Thus, once the CSS has been stripped from the DVD contents by operation of DVD-X-Copy, any number of freely available software programs are able to, and will, make unlimited serial copies of that content -- whether from the DVD-R or the computer hard drive

copy -- without any restrictions. I personally have confirmed this by making multiple copies of a DVD-R originally made using DVD-X-Copy. Attached hereto as Exhibit G is a true and correct copy of a screenshot reflecting the contents of a DVD-R that was made using DVD-X-Copy being serially copied back to my computer hard drive using a third-party software application. By stripping away the CSS protections, DVD-X-Copy leaves each copy it makes vulnerable to unlimited serial copying and distribution.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 9th day of January, 2003.

Robert Schumann